How To | Apply Firewall Policies And Rules

Introduction

This How To Note describes some of the more subtle aspects of dealing with firewall policies and how to apply rules to various traffic flows when using multiple firewall policies.

Which products does it apply to?

This Note applies to the following Allied Telesis routers and managed layer 3 switches:

- AR300, AR400, and AR700 series routers
- AT-8800, Rapier, and Rapier i series switches
- AT-9800 series switches

Related How To Notes

You also may find the following How To Notes useful:

- *How To Configure Some Basic Firewall And VPN Scenarios*
- *How To Configure Some Advanced Features On Your ADSL Router*
- *How To Configure The Firewall Using The Graphical User Interface (GUI)*
- *How To Use Switch Hardware Filters To Enforce Restrictions In A LAN And Take Some Of The Load Off A Firewall*

How To Notes are available from www.alliedtelesis.com/resources/literature/howto.aspx.

Which packet paths are, and are not, subject to firewall scrutiny?

The way the firewall deals with a packet depends on both the ingress and egress interfaces that the packet will use in passing through the router. The conventions are:

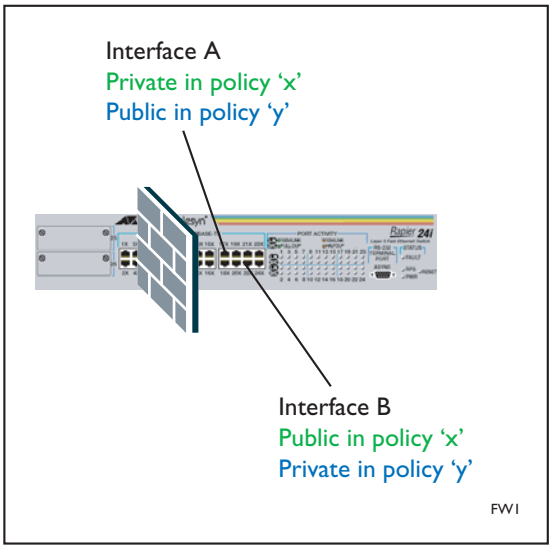
1. a rule affects traffic coming in on the interface it is applied to, when travelling from a public interface to a private interface.
2. a rule affects traffic coming in on the interface it is applied to, when travelling from a private interface to a public interface.
3. a rule **does not** affect traffic coming in on the interface it is applied to, when travelling from a private interface to a private interface.
4. a rule **does not** affect traffic coming in on the interface it is applied to, when travelling from a public interface to a public interface.

How to deal with a case where multiple different policies apply to the same interface

When there are two or more policies attached to the same interface, both policies affect the flow of traffic. What happens if the policies disagree about whether a particular flow should be allowed through the firewall? The rule is:

A flow is only allowed to go through the firewall if all policies agree it is allowed.

For example, consider you have two interfaces, A and B, and two policies, 'x' and 'y'.
In policy 'x', interface A is private and interface B is public.
In policy 'y', interface B is private and interface A is public.



If you have an HTTP flow going from interface A to interface B, policy 'x' allows it, because the traffic is going from the private interface to the public interface, and there are no rules applied to interface A that deny this flow. This same HTTP flow is then checked against the second policy (policy 'y'). From the point of view of policy 'y', the flow is going from a public to a private interface. Hence, policy 'y' will deny this flow. Therefore, we have a disagreement

between the two policies. But the rule is that if any policy denies the flow, the flow must be denied.

To allow the flow through policy 'y' you need to add a rule for **port=80**, using the command:

```
add fire poli=y rule=1 int=a action=allow prot=tcp port=80
```

Note: When a flow or session goes from a private interface through the public interface of a firewall, then the firewall automatically allows reply traffic back in and out through the public interface.

Conventions applied to non-policy interfaces

A router or switch can be configured with several IP interfaces. When the firewall is enabled, various interfaces can be added to various firewall policies. But it is possible for some of the IP interfaces on the device to not be added to any firewall policies. We refer to these as non-policy interfaces.

Non-policy interfaces are generally treated as public interfaces for security purposes. However, there are some subtle differences. The precise conventions are:

1. traffic travelling from a non-policy interface to a private interface is **always** denied.
2. traffic travelling from a private interface to a non-policy interface is **always** denied.
3. traffic travelling from a non-policy interface to a public interface is **always** allowed.
4. traffic travelling from a public interface to a non-policy interface is always allowed **unless** the public interface has a rule defined on it to explicitly deny the particular traffic flow.

The reason for convention 2 is that the network attached to a non-policy interface is deemed to be an unprotected zone, i.e. it is considered that we do not know whether devices connected to the non-policy interface are benign or malign. It is safer not to allow traffic from our private network to be seen by devices attached to the non-policy interface.

Tips, tricks and recommendations regarding the firewall

This section discusses various subtle aspects of the firewall facility. Its aim is to answer some not-so-frequently asked questions—they are very interesting questions all the same!

Is it a good idea to have non-policy interfaces on a device which has the firewall enabled?

In general, it is considered bad practice for there to be any non-policy interfaces. Each policy should have each interface specifically defined as either private or public.

Are there any cases where it IS desirable to have non-policy interfaces on a firewall-enabled device?

Yes, there is one particular case where it is desirable. To understand this case, it is necessary to explain a bit about the operation of the Allied Telesis managed Layer 3 switches. On the Layer 3 switches, if the firewall is enabled, then all packets going to or from a policy interface **must** be passed up to the CPU. But, packets travelling between non-policy interfaces are hardware switched.

Of course, the CPU has a much lower packet forwarding performance than the switching hardware. So, if you know that certain traffic does **not** need to be inspected by the firewall, it is very desirable for that traffic not to be passed to the CPU, but to be hardware switched.

If whole sets of devices on the network are **only** sending internal private traffic, then these devices should be configured on different VLANs to those which require external access. These VLANs should not be configured as firewall interfaces, they should be non-policy interfaces. This will result in traffic between these VLANs being switched in the ASIC, not by the CPU, which results in wirespeed switching between these interfaces.

Because these non-firewall VLANs are treated as public interfaces security-wise, access to and from these should be managed via the use of hardware filters. This is particularly important to prevent unauthorised external access which is not prevented by the firewall. Using hardware filters as opposed to IP filters will mean that traffic for these VLANs is still handled via the ASICs.

Can I configure QoS on a device being used as a firewall?

Yes, you can use software QoS over the WAN link.

Whenever you have a firewall configured on a switch or router, all the packets that enter the switch via firewall interfaces are passed up to the CPU to be processed. This means that packets are going to be software switched by the CPU. In particular, this will mean that the packets will bypass any hardware-based QoS processing that you might have configured. It is therefore generally not recommended to configure hardware-based QoS on a switch that is being used as a firewall device.

How can I restrict traffic that is travelling between two private interfaces?

Packets travelling between private interfaces are never passed to the firewall. If you do want to place some restrictions on the passage of these packets, you need to use another facility. You can do this using IP filters or hardware filters.

How can I restrict traffic that is travelling between two public interfaces?

- You can use IP filters or hardware filters.
- Alternatively, you can add a second policy and make one of the interfaces private in this policy. Then, define rule on this second policy and they will apply to packets passing between these two interfaces.

What are the restrictions governing the inclusion of interfaces in multiple policies?

- A policy must contain at least one private interface and at least one public interface.
- An interface can only be specified as private in one policy.
- An interface can be specified as public in up to two policies.

Can I have more than two policies?

We strongly advise against this as it may affect the integrity of your firewall.

If a policy has more than one rule that matches a particular flow, which one will be applied?

Rules are processed in order from the lowest ID number to the highest number. As soon as a rule has been found which matches a particular flow, then the action of that rule is applied, and no further rules on that policy are considered.

Note that the order in which the rules have been configured does not affect the order in which they are checked. The order of the checking is governed only by the ID number of each rule.

For example, consider the case where a set of firewall commands have been entered in the following order:

```
add fire poli=x rule=5 int=a action=deny prot=tcp port=80
add fire poli=x rule=1 int=a action=deny prot=tcp port=443
add fire poli=x rule=3 int=a action=allow prot=tcp
add fire poli=x rule=2 int=a action=deny prot=tcp port=20
```

The rules are applied numerically. The order in which the firewall checks the rules is:

```
add fire poli=x rule=1 int=a action=deny prot=tcp port=443
add fire poli=x rule=2 int=a action=deny prot=tcp port=20
add fire poli=x rule=3 int=a action=allow prot=tcp
add fire poli=x rule=5 int=a action=deny prot=tcp port=80
```

Hence, the effect of this policy will be as summarised in the following table:

Flow	Allowed or denied?
Secure HTTP/HTTPS (TCP port 443)	Denied. Matches first rule in the list (Rule 1). No further rules are checked, so Rule 3 is never applied for this flow.
FTP (TCP port 20)	Denied. Matches second rule in the list (Rule 2). No further rules are checked, so Rule 3 is never applied for this flow.
Telnet (TCP port 23)	Allowed. Matches third rule in the list (Rule 3). No further rules are checked.
HTTP (TCP port 80)	Allowed. Matches third rule in the list (Rule 3). No further rules are checked, so Rule 5 is never applied. To ensure **port=80** traffic is denied, Rule 5 must come before Rule 3. This means you have to renumber the rules.

If there are multiple policies configured on the firewall, and more than one of the policies has a rule that matches a particular flow, which rule takes precedence?

As discussed on page 2 of this Note, if more than one policy applies to a particular flow, then the flow will only be allowed if all the relevant policies agree to forward it. Otherwise the flow is denied.

How can I block someone from telneting to my router from a private interface using the IP of another private interface?

- You can disable the telnet server using the command **disable telnet server**.
- You can block the traffic with IP or hardware filters.
- You can use the firewall policy **trustprivate** parameter, available in software version 2.6.1 and later.

  The **trustprivate** parameter specifies whether devices connected to the interface are trusted enough to have access to the router or switch via the private interface that is unrestricted by the firewall policy. This parameter may only be specified when **type=private**. (Access to the router or switch by devices connected to public interfaces is always restricted by the firewall.)

  For example, consider an example where two interfaces (A and B) are private interfaces on a firewall policy 'x'. If the hosts on the network attached to interface A **are not** allowed access to the router or switch, but devices connected to interface B **are** allowed access, then the relevant configuration commands would be:

  ```
  create fire poli=x
  add fire poli=x int=a type=private trustprivate=false
  add fire poli=x int=b type=private trustprivate=true
  ```

  The **trustprivate** setting only affects traffic destined for the router or switch itself and does not affect traffic passing through the router or switch.

USA Headquarters | 19800 North Creek Parkway | Suite 200 | Bothell | WA 98011 | USA | T: +1 800 424 4284 | F: +1 425 481 3895
European Headquarters | Via Motta 24 | 6830 Chiasso | Switzerland | T: +41 91 69769.00 | F: +41 91 69769.11
Asia-Pacific Headquarters | 11 Tai Seng Link | Singapore | 534182 | T: +65 6383 3832 | F: +65 6383 3830
www.alliedtelesis.com

C613-16026-00 REV B